UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

BRUCE PARKER, on behalf of himself and all others similarly situated, Plaintiff, v. THE PRUDENTIAL INSURANCE COMPANY OF AMERICA, Defendant.	Case No.: _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff, Bruce Parker ("Plaintiff"), brings this Class Action Complaint ("Complaint") against Defendant, The Prudential Insurance Company of America ("Prudential" or "Defendant"), as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigation, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiff seeks monetary damages and injunctive and declaratory relief in this action, arising from Defendant's failure to safeguard the Personally Identifiable Information[1]

[1] The Federal Trade Commission ("FTC") defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8). To be clear, according to Defendant, not every type of information included in that definition was compromised in the subject data breach.

("Private Information") of its customers and insurance agents, which resulted in unauthorized access to its information systems on May 29 and May 30, 2023 and the compromised and unauthorized disclosure of that Private Information, causing widespread injury and damages to Plaintiff and the proposed Class (defined below) members.

2. Defendant is a Newark, New Jersey-based insurance company, serving customers and working with insurance agents throughout the country.

3. As explained in detail herein, an unauthorized third party accessed one of Defendant's MOVEit Transfer servers and downloaded certain files from the server on May 29, 2023 and May 30, 2023 ("Data Breach").[2]

4. As a result of the Data Breach, which Defendant failed to prevent, the Private Information of Defendant's customers, including Plaintiff and the proposed Class members, were stolen.

5. For customers, the exposed information includes one or more of the following: Social Security number, first and last name, date of birth, zip code, state of residence and phone number.

6. Defendant's investigation concluded that the Private Information compromised in the Data Breach included Plaintiff's and approximately 320,840 other individuals' information (together, "Consumers").[3]

7. Defendant's failure to safeguard Consumers' highly sensitive Private Information as exposed and unauthorizedly disclosed in the Data Breach violates its common law duty and Defendant's implied contract with its Consumers to safeguard their Private Information.

---

[2] *See* July 31, 2023 Letter to Bruce Parker (the "Notice"), attached as ***Exhibit A***.
[3] https://apps.web.maine.gov/online/aeviewer/ME/40/e2a5ab4c-3947-4a2e-a9fe-b58eec80686c.shtml (last accessed Aug. 15, 2023).

8. Plaintiff and Class members now face a lifetime risk of identity theft due to the nature of the information lost, including Social Security numbers, which they cannot change, and which cannot be made private again.

9. Defendant's harmful conduct has injured Plaintiff and Class members in multiple ways, including: (i) the lost or diminished value of their Private Information; (ii) costs associated with the prevention, detection, and recovery from identity theft, tax fraud, and other unauthorized use of their data; (iii) lost opportunity costs to mitigate the Data Breach's consequences, including lost time; and (iv) emotional distress associated with the loss of control over their highly sensitive Private Information.

10. Defendant's failure to protect Consumers' Private Information has harmed and will continue to harm over 320,000 of Defendant's Consumers, causing Plaintiff to seek relief on a class wide basis.

11. On behalf of himself and the Classes preliminarily defined below, Plaintiff brings causes of action against Defendant for negligence, negligence *per se*, breach of implied contract, breach of fiduciary duty, breach of confidence, and unjust enrichment, seeking an award of monetary damages and injunctive and declaratory relief, resulting from Defendant's failure to adequately protect their highly sensitive Private Information.

PARTIES

12. Plaintiff is, and at all times mentioned herein was, an individual resident and citizen of the state of California.

13. Plaintiff provided Private Information to Defendant on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect his Private Information.

14. If Plaintiff had known that Defendant would not adequately protect his Private Information, he would not have allowed Defendant to maintain this sensitive Private Information.

15. Defendant is a New Jersey corporation with its headquarters and principal place of business at 751 Broad Street, Newark, New Jersey 07102.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

17. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District. Defendant has sufficient contacts in New Jersey, as it conducts a significant amount of its business in the state of New Jersey.

18. Venue is proper under 18 U.S.C § 1391(b)(2) because a substantial part of the events or omissions giving rise to the Plaintiff's claims occurred in this District.

FACTUAL BACKGROUND

Defendant's Business

19. Defendant is a Newark, New Jersey-headquartered insurance company.

20. Plaintiff and Class members are current or former Consumers who provided their Private Information to Defendant.

21. To obtain Defendant's services, Consumers, including Plaintiff and Class members, were required to provide sensitive and confidential Private Information, including their names,

Social Security numbers, dates of birth, zip codes, states of residence, addresses, and other sensitive information, that would be held by Defendant in its computer systems.

22. The information held by Defendant at the time of the Data Breach included the unencrypted Private Information of Plaintiff and Class members.

23. Upon information and belief, Defendant made promises and representations to its Consumers that the Private Information collected would be kept safe and confidential, the privacy of that information would be maintained, and Defendant would delete any sensitive information after it was no longer required to maintain it.

24. Indeed, Defendant acknowledges the importance of keeping Personal Information safe in its own Privacy Policy, which states: "Prudential values your trust and respects your privacy." It also states:

> **How we protect your privacy**
>
> We maintain physical, electronic, and procedural safeguards to protect your personal information. The people who are authorized to have access to your personal information need it to do their jobs, and we require them to keep that information secure and confidential.[4]

25. Plaintiff and Class members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

26. Plaintiff and Class members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiff and Class members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of

[4] https://www.prudential.com/links/privacy-center (last accessed Aug. 15, 2023).

this information. Plaintiff and Class members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

27. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class members from involuntary disclosure to third parties. Defendant has a legal duty to keep Consumers' Private Information safe and confidential.

28. Defendant had obligations under the FTC Act, contract, industry standards, and representations made to Plaintiff and Class members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

29. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class members' Private Information. Without the required submission of Private Information, Defendant could not perform the services it provides.

30. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class members' Private Information from disclosure.

The Data Breach

31. On or about July 31, 2023, Defendant began notifying Consumers of the Data Breach, informing them in a Notice:

> On or about May 31, 2021, Progress Software, the provider of MOVEit Transfer software disclosed a vulnerability in their software that had been exploited by an unauthorized third party. PBI[5] utilizes MOVEit in the regular course of our business operations to security transfer files, including with Prudential and our other

[5] According to Defendant, Pension Benefit Information, LLC ("PBI") "provides regulatory compliance and operational support services for insurance companies, pension funds, and other organizations, including, on a limited basis, for The Prudential Insurance Company of America ("Prudential"). Prudential provides payment services for monthly retirement payments on behalf of the Western Conference of Teamsters Pension Trust Fund, as well as other entities." *See* Notice.

> customers. PBI promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on our systems. Through the investigation, we learned that the third party accessed one of our MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded data. We then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. We recently completed this review and shared the findings with our impacted customers.

32. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiff and Class members, such as encrypting the information or deleting it when it is no longer needed, causing the exposure of Private Information.

33. The attacker accessed and acquired files in Defendant's computer systems containing unencrypted Private Information of Plaintiff and Class members, including their Social Security number, first and last name, date of birth, zip code, state of residence and telephone number.

34. Plaintiff's and Class members' Private Information was accessed and stolen in the Data Breach.

35. Plaintiff further believes his Private Information, and that of Class members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' Private Information.

36. As a condition to obtain insurance services from Defendant, Plaintiff and Class members were required to give their sensitive and confidential Private Information to Defendant.

37. Defendant retains and stores this information and derives a substantial economic benefit from the Private Information that it collects. But for the collection of Plaintiff's and Class members' Private Information, Defendant would be unable to perform its services.

38. By obtaining, collecting, and storing the Private Information of Plaintiff and Class members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Private Information from disclosure.

39. Plaintiff and Class members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

40. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiff and Class members.

41. Upon information and belief, Defendant made promises to Plaintiff and Class members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information.

42. Defendant's negligence in safeguarding the Private Information of Plaintiff and Class members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

Defendant Knew or Should Have Known of the Risk of a Cyber Attack Because Entities in Possession of Private Information are Particularly Suspectable to Cyber Attacks.

43. Data thieves regularly target entities like Defendant due to the highly sensitive information that they maintain. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

44. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities like Defendant that collect and store Private Information and other sensitive information, preceding the date of the Data Breach.

45. In light of recent high profile data breaches at other industry-leading companies, including, *e.g.*, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the Private Information that it collected and maintained would be targeted by cybercriminals.

46. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class members from being compromised.

47. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to over two *million* individuals' detailed Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

48. In its Notice, Defendant says PBI "is offering you access to 24 months of complimentary credit monitoring and identity restoration services through Kroll."[6] This is wholly inadequate to compensate Plaintiff and Class members, as it fails to account for the multiple years of ongoing identity theft and financial fraud commonly faced by victims of data breaches and other unauthorized disclosures. It also fails to provide sufficient compensation to Plaintiff and Class

[6] *See* Notice.

members for the unauthorized release and disclosure of their Private Information. Moreover, once the identity theft service expires, Plaintiff and Class members will be forced to pay out of pocket for necessary identity monitoring services.

49. The offering of identity theft protection establishes that Plaintiff's and Class members' sensitive Private Information *was* in fact affected, accessed, compromised, and exfiltrated from Defendant's computer systems. Moreover, the offer indicates that Defendant recognizes that Plaintiff and Class members are at a present and continuing risk of identity theft and fraud as a result of the Data Breach.

50. The injuries to Plaintiff and Class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class members.

51. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class members are long lasting and severe. Once Private Information is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

52. As an insurance entity in possession of its Consumers' Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class members because of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

Defendant Fails to Comply with FTC Guidelines

53. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

54. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[7]

55. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[8]

56. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

57. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and

[7] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Aug. 4, 2023).
[8] *Id.*

appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

58. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

59. Defendant failed to properly implement basic data security practices.

60. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Consumers' Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

61. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the Private Information of its Consumers; Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

Defendant Owed Plaintiff and Class Members a Duty to Safeguard their Private Information.

62. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing,

safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class members.

63. Defendant owed a duty to Plaintiff and Class members to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees and others who accessed Private Information within its computer systems on how to adequately protect Private Information.

64. Defendant owed a duty to Plaintiff and Class members to implement processes that would detect a compromise of Private Information in a timely manner.

65. Defendant owed a duty to Plaintiff and Class members to act upon data security warnings and alerts in a timely fashion.

66. Defendant owed a duty to Plaintiff and Class members to disclose in a timely and accurate manner when and how the Data Breach occurred.

67. Defendant owed a duty of care to Plaintiff and Class members because they were foreseeable and probable victims of any inadequate data security practices.

The Data Breach Increases Plaintiff's and Class Members' Risk of Identity Theft.

68. The unencrypted Private Information of Plaintiff and Class members will end up (if it has not already ended up) for sale on the dark web, as that is the *modus operandi* of hackers.

69. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class members.

70. Simply put, unauthorized individuals can easily access the Private Information of Plaintiff and Class members because of the Data Breach.

71. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

72. Plaintiff's and Class members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and Class members and to profit from their misfortune.

Loss of Time to Mitigate the Risk of Identity Theft and Fraud

73. As a result of the recognized risk of identity theft, when a data breach occurs and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm.

74. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class members must, as Defendant's Notice encourages them to, "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors for the next twelve to twenty-four months and

to report suspected identify theft incidents to the insurance company."[9] They must also monitor their financial accounts for many years to mitigate the risk of identity theft.

75. Plaintiff and Class members have spent, and will spend additional time in the future, on a variety of prudent actions, such as changing passwords and resecuring their own computer systems.

76. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[10]

77. Plaintiff's mitigation efforts are also consistent with the steps the FTC recommends data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[11]

78. And for those Class members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

---

[9] *See* Notice.

[10] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf (last accessed Aug. 4, 2023).

[11] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last accessed Aug. 4, 2023).

Diminution of Value of Private Information.

79. Private Information is valuable property.[12] Its value is axiomatic, considering the value of Big Data in corporate America and that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates, beyond doubt, that Private Information has considerable market value.

80. The Private Information stolen in the Data Breach is significantly more valuable than the loss of, say, credit card information in a large retailer data breach. Victims affected by those retailer breaches could avoid much of the potential future harm by simply cancelling credit or debit cards and obtaining replacements. The information stolen in the Data Breach—most notably name and Social Security number—is difficult, if not impossible, to change.

81. This kind of data, as one would expect, demands a much higher price on the dark web. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information… [is] worth more than 10x on the black market."[13]

82. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[14]

83. An active and robust legitimate marketplace for Private Information also exists. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public

---

[12] *See* GAO Report.

[13] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hackpersonal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Aug. 4, 2023).

[14] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private Information") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[15,16] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[17]

84. As a result of the Data Breach, Plaintiff's and Class members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

85. The fraudulent activity resulting from the Data Breach may not come to light for years.

86. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class members are incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

87. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to millions of individuals' detailed Private Information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

---

[15] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last accessed Aug. 4, 2023).
[16] https://datacoup.com/ (last accessed Aug. 4, 2023).
[17] https://www.thepennyhoarder.com/make-money/nielsen-panel/#:~:text=Sign%20up%20to%20join%20the,software%20installed%20on%20your%20computer (last accessed Aug. 4, 2023).

88. The injuries to Plaintiff and Class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class members.

The Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary.

89. Given the type of targeted attack in this case, the sophisticated criminal activity, the volume of data compromised in this Data Breach, and the sensitive type of Private Information involved in this Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

90. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Private Information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

91. Consequently, Plaintiff and Class members are at an increased risk of fraud and identity theft for many years into the future.

92. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class member. This is a reasonable and necessary cost to monitor and protect Class members from the risk of identity theft resulting from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class members would not need to bear, but for Defendant's failure to safeguard their Private Information.

Loss of the Benefit of the Bargain

93. Furthermore, Defendant's poor data security deprived Plaintiff and Class members of the benefit of their bargain. When agreeing to pay Defendant for the provision of its services, customers reasonably understood and expected that they were, in part, paying for the service and necessary data security to protect the Private Information when, in fact, Defendant did not provide the expected data security. Similarly, when providing their Personal Information to Defendant in order to work with Defendant, insurance agents reasonably understood that Defendant would provide the necessary data security to protect the Private Information when, in fact, it did not. Accordingly, Plaintiff and Class members received services (for customers) and compensation (for insurance agents) that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Plaintiff's Experience

94. Plaintiff obtained insurance services from Defendant. To obtain these insurance services, he was required to provide his Private Information to Defendant.

95. Upon information and belief, at the time of the Data Breach— on May 29 and May 30, 2023—Defendant retained Plaintiff's Private Information in its system.

96. Plaintiff is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

97. Plaintiff received a Notice from Defendant on or about July 31, 2023. According to the Notice, Plaintiff's Private Information was improperly accessed and obtained by unauthorized

third parties, including his name, Social Security number, date of birth, zip code, state of residence, and telephone number.

98. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including checking his bills and accounts to make sure they were correct. Plaintiff has spent significant time dealing with the Data Breach, valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

99. As a result of the Data Breach, Plaintiff fears for his personal financial security and uncertainty over what Personal Information was revealed in the Data Breach. He is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

100. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

101. As a result of the Data Breach, Plaintiff is presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

102. Plaintiff has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

103. Pursuant to Federal Rules of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4), Plaintiff brings this action on behalf of himself and on behalf of all members of the proposed Nationwide Class and Florida Subclass (together, the "Class" or "Classes")) defined as:

Nationwide Class: All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach reported to have occurred on or about May 29 and May 30, 2023.

104. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

105. Plaintiff reserves the right to amend the definition of the Class or add a Class or Sub-class if further information and discovery indicate that the definition of the Class should be narrowed, expanded, or otherwise modified.

106. **Numerosity**: The Class members are so numerous that joinder of all members is impracticable, if not completely impossible. Approximately three hundred twenty thousand, eight hundred forty (320,840) individuals were affected by the of the Data Breach. The Class is apparently identifiable within Defendant's records, and Defendant has notified these individuals. *See, e.g.*, Notice.

107. Common questions of law and fact exist as to all Class members and predominate over any questions affecting solely individual Class members. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, are the following:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class members;

b. Whether Defendant had respective duties not to disclose the Private Information of Plaintiff and Class members to unauthorized third parties;

c. Whether Defendant had respective duties not to use the Private Information of Plaintiff and Class members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class members;

e. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

f. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

g. Whether Plaintiff and Class members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct; and

h. Whether Plaintiff and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

108. **Typicality**: Plaintiff's claims are typical of those of the other Class members because Plaintiff, like every other Class member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Classes.

109. This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class members uniformly and Plaintiff's challenge

of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

110. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of Class members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Class members. Plaintiff seeks no relief that is antagonistic or adverse to Class members and the infringement of the rights and the damages he has suffered are typical of other Class members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

111. **Superiority**: Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that millions of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

112. The nature of this action and the nature of laws available to Plaintiff and Class members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class member with superior financial and legal resources;

the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

113. Adequate notice can be given to Class members directly using information maintained in Defendant's records.

114. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

a. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

b. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

c. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

d. Whether Defendant's failure to institute adequate protective security measures amounted to breach of an implied contract;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations and measures recommended by data security experts would have reasonably prevented the Data Breach.

CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

115. Plaintiff restates and realleges all of the allegations stated above as if fully set forth herein.

116. Defendant requires its Consumers, including Plaintiff and Class members, to submit non-public Private Information in the ordinary course of providing insurance services.

117. Defendant gathered and stored the Private Information of Plaintiff and Class members as part of its business of soliciting customers, which solicitations and services affect commerce.

118. Plaintiff and Class members entrusted Defendant with their Private Information with the understanding that Defendant would safeguard their information.

119. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class members could and would suffer if the Private Information were wrongfully disclosed.

120. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

121. Defendant owed a duty of care to Plaintiff and Class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

122. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its Consumers. That special relationship arose because Plaintiff and Class members entrusted Defendant with their confidential Private Information, a necessary part of being customers of Defendant.

123. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

124. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

125. Defendant breached its duties, thus was negligent, by failing to use reasonable measures to protect Class members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, (a) failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information; (b) failing to adequately monitor the security of their networks and systems; and (c) allowing unauthorized access to Class members' Private Information.

126. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly considering Defendant's inadequate security practices.

127. It was foreseeable that Defendant's failure to use reasonable measures to protect Class members' Private Information would result in injury to Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

128. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class members could and would suffer if the Private Information were wrongfully disclosed.

129. Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and Class members, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

130. It was therefore foreseeable that the failure to adequately safeguard Class members' Private Information would result in one or more types of injuries to Class members.

131. Plaintiff and Class members had no ability to protect their Private Information that was in, and likely remains in, Defendant's possession.

132. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

133. Defendant's duty extended to protecting Plaintiff and Class members from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement

(Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

134. Defendant has admitted that the Private Information of Plaintiff and Class members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

135. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class members, the Private Information of Plaintiff and Class members would not have been compromised.

136. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and Class members and the harm, or risk of imminent harm, suffered by Plaintiff and Class members. The Private Information of Plaintiff and Class members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

137. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of their Private Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

138. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

139. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

140. Plaintiff and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

141. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class members.

COUNT II
Negligence *Per Se*
(On behalf of Plaintiff and the Nationwide Class)

142. Plaintiff restates and realleges all of the allegations stated above as if fully set forth herein.

143. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

144. Defendant breached its duties to Plaintiff and Class members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

145. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se.*

146. The injuries to Plaintiff and Class members resulting from the Data Breach were directly and indirectly caused by Defendant's violation of the statute described herein.

147. Plaintiff and Class members were within the class of persons the Federal Trade Commission Act were intended to protect and the type of harm that resulted from the Data Breach was the type of harm the statue was intended to guard against.

148. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiff and Class members, Plaintiff and Class members would not have been injured.

149. The injuries and harms suffered by Plaintiff and Class members were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties and that Defendant's breach would cause Plaintiff and Class members to experience the foreseeable harms associated with the exposure of their Private Information.

150. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class members have suffered injuries and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

151. Plaintiff restates and realleges all of the allegations stated above as if fully set forth

herein.

152. Defendant offered to provide services to its Consumers, including Plaintiff and Class members, in exchange for payment (for customers).

153. Defendant also required Plaintiff and the Class members to provide Defendant with their Private Information to receive services from Defendant.

154. In turn, Defendant impliedly promised to protect Plaintiff's and Class members' Private Information through adequate data security measures.

155. Customers accepted Defendant's offer by providing Private Information to Defendant in exchange for receiving Defendant's services, and then by paying for and receiving the same.

156. Plaintiff and Class members would not have entrusted their Private Information to Defendant but-for the above-described agreement with Defendant.

157. Defendant materially breached its agreement(s) with Plaintiff and Class members by failing to safeguard such Private Information, violating industry standards necessarily incorporated in the agreement.

158. Plaintiff and Class members have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

159. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose on each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract along

with its form.

160. Defendant's conduct as alleged herein also violated the implied covenant of good faith and fair dealing inherent in every contract.

161. The losses and damages Plaintiff and Class members sustained as described herein were the direct and proximate result of Defendant's breach of the implied contracts with them, including breach of the implied covenant of good faith and fair dealing.

COUNT IV
Breach Of Fiduciary Duty
(On Behalf Of Plaintiff And the Class)

162. Plaintiff restates and realleges all of the allegations stated above as if fully set forth herein.

163. In providing their PII, directly or indirectly, to Defendant, Plaintiff and Class members justifiably placed a special confidence in Defendant to act in good faith and with due regard to interests of Plaintiff and class members to safeguard and keep confidential that PII.

164. Defendant accepted the special confidence Plaintiff and Class members placed in it, as evidenced by its assertion that it is committed to protecting the privacy of Plaintiff's and Class Members' personal information as detailed in its Privacy Policy.

165. In light of the special relationship between Defendant and Plaintiff and Class members, whereby Defendant became a guardian of Plaintiff's and Class members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for the benefit of its customers, including Plaintiff and Class members, for the safeguarding of Plaintiff and Class member's PII.

166. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of its relationship with Defendants' customers, in particular, to keep

secure the PII of its customers.

167. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to protect the integrity of the systems containing Plaintiff's and Class member's PII.

168. Defendant breached its fiduciary duties to Plaintiff and class members by otherwise failing to safeguard Plaintiff's and Class members' PII.

169. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and class members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

170. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT IV
Breach Of Confidence
(On Behalf Of Plaintiff And the Class)

171. Plaintiff restates and realleges all of the allegations stated above as if fully set forth herein.

172. At all times during Plaintiff and Class members' interactions with Defendant, Defendant was fully aware of the confidential, novel, and sensitive nature of Plaintiff's and the Class members' PII that Plaintiff and Class members provided to Defendant.

173. As alleged herein and above, Defendant's relationship with Plaintiff and Class members was governed by expectations that Plaintiff and Class members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

174. Plaintiffs and Class members provided their respective PII to Defendant, directly or indirectly, with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized parties.

175. Plaintiffs and Class members also provided their respective PII to Defendant with the explicit understanding that Defendant would take precautions to protect that PII from unauthorized disclosure, such as following basic principles of information security practices.

176. Defendant voluntarily received in confidence Plaintiff and Class members' PII with the understanding that the PII would not be disclosed or disseminated to the public or any unauthorized third parties.

177. Due to Defendant's failure to prevent, detect, and/or avoid the Data Breach from occurring by, *inter alia*, failing to follow best information security practices to secure Plaintiffs' and Class members' PII, Plaintiffs' and Class members' PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class members' confidence, and without their express permission.

178. But for Defendant's disclosure of Plaintiffs' and Class members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class members' PII, as well as the resulting damages.

179. The injury and harm Plaintiffs and Class members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and Class members' PII.

Defendant knew or should have known their security systems were insufficient to protect the PII that is coveted by thieves worldwide. Defendant also failed to observe industry standard information security practices.

180. As a direct and proximate cause of Defendant's conduct, Plaintiffs and Class members suffered damages as alleged above.

COUNT V
Unjust Enrichment / Quasi Contract
(On Behalf Of Plaintiff And the Class)

181. Plaintiff restates and realleges all of the allegations stated above as if fully set forth herein.

182. Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable PII. In so conferring this benefit, Plaintiff and Class Members understood that part of the benefit Defendant derived from the PII would be applied to data security efforts to safeguard the PII.

183. Defendant appreciated that Plaintiff and Class Members were conferring a benefit upon it and accepted that monetary benefit.

184. Acceptance of the benefit under the facts and circumstances described herein make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

185. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

186. Defendant acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

187. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

188. Plaintiff and Class Members have no adequate remedy at law.

189. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

190. As a direct and proximate result of Defendant's conduct, Plaintiff and Class

Members have suffered and will continue to suffer other forms of injury and/or harm.

191. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

D. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. Prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. Requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local

laws;

iii. Requiring Defendant to delete, destroy, and purge the PII of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. Requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. Prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. Requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. Requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. Requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. Requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of

Defendant's systems;

x. Requiring Defendant to conduct regular database scanning and securing checks;

xi. Requiring Defendant to establish an information security training program that includes at least annual information security training for all patients, with additional training to be provided as appropriate based upon the patients' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. Requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. Requiring Defendant to implement a system of tests to assess its respective patients' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing patients' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. Requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. Requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and

xvi. Requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment.

E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

F. Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiff and the Class;

G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

H. For an award of punitive damages, as allowable by law;

I. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

J. Pre- and post-judgment interest on any amounts awarded; and

K. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: August 15, 2023

Respectfully submitted,

/s/ Vicki J. Maniatis
Vicki J. Maniatis NJ - 001321994
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza, Suite 500
Garden City, New York 11530
Tel.: (865) 412-2700
vmaniatis@milberg.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN LLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

Andrew J. Shamis, Esq.*
SHAMIS & GENTILE P.A.
ashamis@shamisgentile.com
14 NE 1st Ave., Suite 705
Miami, Florida 33132
Telephone: 305-479-2299

KOPELOWITZ OSTROW FERGUSON WEISELBERG GILBERT
Jeff Ostrow*
Kristen Lake Cardoso*
Steven Sukert*
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Tel: (954) 525-4100
ostrow@kolawyers.com
cardoso@kolawyers.com
sukert@kolawyers.com

*pro hac vice forthcoming

Counsel for Plaintiff and the Class